IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts CIO-IT Security-09-48

Revision 5

August 25, 2020

Office of the Chief Information Security Officer

IMPORTANT!

This guide defines security and privacy requirements for GSA IT acquisition contracts involving externally hosted contractor information systems that do not connect to the GSA network; information systems hosted in GSA facilities that directly connect to the GSA network; cloud information systems; or mobile applications. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract requirements to be placed in-line within a statement of work for each system type. Alternatively, this entire document can be incorporated into the statement of work or contract.

NOTE: Throughout this guide there are highlighted SELECT statements. The requirements office, in coordination with the contracting officer, will complete the selections prior to their incorporation into a contract or statement of work. See example below for the intended use of the SELECT statements.

The guide text states:

1. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."*

The requirements office in coordination with the contracting officer would determine for the specific SOW/contract being prepared whether the contractor or the Government was responsible for the independent assessment and change the statement accordingly. For example, if the contractor is required to provide an independent assessment the statement would state:

1. At the Moderate impact level and higher, the contractor is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."*

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – November 6, 2009		
1	Bo Berlas	Minor Changes to GSA 800-53 R3 Control Tailoring workbook in Appendix A	GSA 800-53 Control Tailoring Workbook Update	17
		Revision 2 – November 7, 2014		
1	John Sitcharing/ Blanche Heard	Minor changes to verbiage regarding Penetration Testing	Update Penetration Testing verbiage	9
2	John Sitcharing/ Blanche Heard	CISO mandated change in Penetration Testing requirement/ naming conventions based on consolidation efforts	CISO Mandate	Entire document
		Revision 3 – February 2, 2017		
1	Bo Berlas	Added Essential Security controls to Section 2	Security Controls Update	9
2	Bo Berlas	Added sections 3-5	Updated to Provide Requirements for Internal Systems, Cloud Systems, and Mobile Applications	22-55
		Revision 4 – January 25, 2018		
1	Bryon Feliksa/ John Klemens	Incorporated security references from MV 16-01 and additional references. Added a section on LiSaaS, Privacy controls, and updated Privacy and other sections to align with GSA policy and procedures.	Incorporate MV 16-01 and consolidate GSA Cybersecurity and Privacy Guidance.	Throughout
		Revision 5 – August 25, 2020		
1	Desai, Klemens, Speidel	Incorporated NDAA/FAR clauses that prohibit the acquisition from covered entities. Added information on coordinating NDAs with OGC and NDA templates. Updated to reflect LiSaaS and External Information System Monitoring guides. Updated guidance regarding a number of controls and deliverables.	Incorporate requirements from the NDAA and FAR, coordination with OGC on NDAs, and updated GSA guidance.	Throughout
2	Berlas, Speidel, Desai, Klemens	Added section on Nonfederal System and Organizations, revised Internal Information Systems definition. Clarified the provision of deliverables.	Incorporate requirements from NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”	Sections 1 and 7

APPROVAL

IT Security Procedural Guide 09-48, *"Security and Privacy Requirements for IT Acquisition Efforts,"* Revision 5, is hereby approved for distribution.

X DocuSigned by: Bo Berlas ED717926161544E...

Bo Berlas
GSA Chief Information Security Officer

This guide will be available on the OCISO Webpage and GSA.gov when revised.

Table of Contents

1 Introduction

The U.S. General Services Administration (GSA) must provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by GSA, another agency, contractor, or other source. The Federal Information Security Modernization Act of 2014 (FISMA of 2014) describes Federal agency security and privacy responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." This includes services which are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions. Agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency, information systems used or operated by an agency or other organization on behalf of an agency.

Office of Management and Budget (OMB) Memorandum M-14-04 asserts that agencies are responsible for ensuring information technology acquisitions comply with the information technology security requirements in FISMA of 2014, OMB's implementing policies including OMB Circular A-130 and guidance and standards from the National Institute of Standards and Technology (NIST).

1.1 Scope

This guide provides security and privacy requirements for the GSA information system types outlined below:

- **External Information Systems.** External information systems reside in contractor facilities and typically do not connect to the GSA network. External information systems may be government owned and contractor operated or contractor owned and operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
- **Internal Information Systems.** Internal information systems reside on premise in GSA facilities and may connect to the GSA network. Internal systems are operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
- **Low Impact Software as a Service (LiSaaS) Systems.** LiSaaS systems must adhere to GSA IT Security Procedural Guide 16-75, "*Low Impact Software as a Service (SaaS) Authorization Process*." LiSaaS systems are cloud applications that are implemented for a limited duration, involve low or very low/negligible risk and would cause limited harm to GSA, and cost less than $100,000 annually to deploy.
- **Cloud Information Systems**. Includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or SaaS. The service offering must be FedRAMP authorized, in-process, or ready; see Section 5 for additional details.
- **Mobile Application.** A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer.

- **Nonfederal Systems and Organizations**. A system or organization: (1) when Controlled Unclassifed Information (CUI) is resident in a nonfederal system and organization; (2) not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency[1]; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

1.2 Purpose

The purpose of this document is to define and establish consistent security and privacy requirements for GSA IT acquisition contracts involving externally hosted information systems that do not connect to the GSA network; information systems hosted in GSA facilities that may connect to the GSA network; LiSaaS systems, cloud information systems; mobile applications; and nonfederal systems with CUI. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract language to be placed in-line within a statement of work for each system type. The security and privacy requirements identified in this guide will ensure compliance with the appropriate provisions of FISMA of 2014, OMB Circular A-130, and NIST Special Publication (SP) 800-53, Revision 4.

2 External Information Systems – IT Security and Privacy Requirements

2.1 Required Policies and Regulations for GSA Contracts

Federal Laws, Regulations, and Guidance:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "*Responsibilities for Federal Information Systems Standards*"
- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- HSPD 12, "*Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*"
- OMB Circular A-130, "*Managing Information as a Strategic Resource*"
- OMB M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)*"
- OMB M 14-03, "*Enhancing the Security of Federal Information and Information Systems*"
- OMB M-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications*"
- OMB M-15-13, "*Policy to Require Secure Connections across Federal Websites and Web Services*"

[1] Nonfederal organizations that collect or maintain information on behalf of a federal agency or that use or operate a system on behalf of an agency, must comply with the requirements in FISMA of 2014, including the requirements in FIPS 200 and the security controls in NIST SP 800-53. (See [44 USC 3554] (a)(1)(A) and Section 2.1 for referenced documents).

- OMB M-17-12, "*Preparing for and Responding to a Breach of Personally Identifiable Information*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*"
- FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"
- NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*"
- NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-53A, Revision 4, *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*"
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-122, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.3, "*Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2200.1, "*GSA Privacy Act Program*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

The GSA policies listed in this paragraph must be followed, if applicable.

- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2104.1, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, "*Mandatory Use of Personal Identity Verification (PIV) Credentials*"

GSA Procedural Guides:

GSA IT Procedural Guides are guidance, unless required by a GSA Directive/Policy, in which case usage is mandatory.

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

2.2 GSA Security Compliance Requirements

FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems*," is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Information systems supporting GSA must meet the minimum security and privacy requirements through the use of security controls in accordance with NIST Special Publication 800-53, Revision 4 (hereafter described as NIST 800-53), *"Security and Privacy Controls for Federal Information Systems and Organizations."*

To comply with the Federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* and then the contractor shall apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are available in the GSA Control Tailoring Workbook referenced in Appendix A of this document.

The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems.

2.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The following table identifies essential security controls from the respective baselines to highlight their importance and ensure they are implemented. The Contractor shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security

Officer for review and approval before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
AC-2	Account Management	L, M, H	
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses from internal users/systems to the external information system must be routed through GSA's managed network access control points, subjecting them to security monitoring.
AU-2	Audit Events	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable GSA IT Security Technical Hardening Guides (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log. For technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA S/SO or Contractor to be approved and accepted by the GSA AO shall be used.
CM-6	Configuration Settings	L, M, H	Information systems, including vendor owned/operated systems on behalf of GSA, shall configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as reviewed and accepted by the GSA AO.
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Cloud Infrastructure as a Service (IaaS) architectures shall implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecom Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H	All information systems shall implement multi-factor authentication for privileged accounts.

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	L, M, H	All information systems must implement multi-factor authentication for non-privileged accounts.
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: Cryptographic Module Validation Program Validated Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.
PL-8	Information Security Architecture	M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.
RA-5	Vulnerability Scanning	L, M, H	All systems must complete the following vulnerability scans: ○ Weekly authenticated scans of operating systems (OS)-including databases ○ Monthly unauthenticated scans of web applications ○ Annual authenticated scans of web applications The most recent vulnerability scanning results shall be provided to GSA together with the quarterly POA&M submission.
SA-22	Unsupported System Components	GSA Required	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on GSA's Enterprise Architecture IT Standards List.

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption. Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains. (see Binding Operational Directive (BOD) 18-01, Enhance Email and Web Security). SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."*
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms
SC-17	PKI Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation,"* and NIST Special Publications 800-32 and 800-63.
SC-18	Mobile Code	M, H	
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	L, M, H	**Systems that process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Authenticators (e.g., passwords, tokens, keys, certificates, hashes, etc.), and other sensitive data as determined by the AO, shall encrypt that data everywhere (i.e., at file level, database level, at rest, and in transit (see SC-8(1)). For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption or tokenization is also acceptable. For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption.** Encryption algorithms shall be FIPS-approved with FIPS-validated encryption modules.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, critical/very high vulnerabilities for Internet-accessible IP addresses must be remediated within 15 days, for all other assets critical/very high vulnerabilities must be remediated within 30 days; High vulnerabilities must be remediated within 30 days; Moderate vulnerabilities must be remediated within 90 days.
SI-3	Malicious Code Protection	L, M, H	
SI-4	Information System Monitoring	L, M, H	
SI-10	Information Input Validation	M, H	All system accepting input from end users must validate the input in accordance to industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security,"* and OWASP Top 10 Web Application Security Vulnerabilities.
AR-2	Privacy Impact and Risk Assessment	See note below	The contractor shall conduct a Privacy Threshold Assessment (PTA) and, if applicable, a Privacy Impact Assessment (PIA) identifying the categories of information and addressing potential risks to PII. The contractor also shall coordinate with the GSA Privacy Office concerning these documents.
AR-8	Accounting of Disclosures	See note below	The contractor shall keep an accurate accounting of disclosures of information held in any system of records under its control.

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
TR-2	System of Records Notices and Privacy Act Statements	See note below.	The contractor shall coordinate with the GSA Privacy Office to ensure System of Records Notices (SORNs) and Privacy Act notices on forms that collect Personally Identifiable Information (PII) are established and kept current.
UL-1	Internal Use	See note below	The contractor shall ensure that PII is shared internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
UL-2	Information Sharing with Third Parties	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure PII is shared in accordance with GSA requirements and agreements with third parties.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

2.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 2 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk,*" provide guidelines for performing the A&A process. The Contractor system/application must have a valid assessment and authorization, known as an Authority to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) when significant changes are made to the system, and as specified in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk,*" and the guides for GSA's other A&A processes referenced therein.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following A&A documentation:

    - System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems*" and completed in accordance with GSA SSP requirements and templates. The SSP shall include as appendices required policies and procedures across 17 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Security Agreements (in agreement with NIST Special

Publication 800-47, *"Security Guide for Interconnecting Information Technology Systems"*). The SSP shall include; as an appendix, a completed GSA Control Tailoring Workbook (CTW) identified in Appendix A of this guide. The column in the CTW titled "Vendor/Contractor Defined Values" shall be used to document all contractor implemented parameter settings that differ from the GSA Defined Value and the Vendor/Contractor defined value when the value is deferred to the Vendor/Contractor. GSA's approval will be documented in the CTW column titled "GSA Approval of Vendor/Contractor Defined Values."

- Contingency Plan completed in agreement with NIST Special Publication 800-34 and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
- Business Impact Assessment completed in agreement with NIST Special Publication 800-34 and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
- Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*
- Incident Response Plan completed in agreement with NIST Special Publication 800-61, "Computer Security Incident Handling Guide" and GSA IT Security Procedural Guide 01-02, "*Incident Response*."
- Incident Response Test Report completed in agreement NIST Special Publication 800-61, "Computer Security Incident Handling Guide" and GSA IT Security Procedural Guide 01-02, "*Incident Response*."
- Configuration Management Plan completed in agreement with GSA IT Security Procedural Guide 01-05, "*Configuration Management*."
- Plan of Action & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."*
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all Internet accessible, all FIPS 199 High, and all High Value Asset (HVA) information systems. These systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37, Revision 2, " *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,"* and CIO IT Security 06-30, "*Managing Enterprise Cybersecurity Risk*" or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program*" that is reviewed and accepted by the GSA CISO.

3. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."*
4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."* Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.
5. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."* Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.
6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. Vulnerabilities must be mitigated as follows:

    (1) For Internet-accessible IP addresses
        (a) Any Critical (Very High) scan vulnerabilities must be remediated within 15 days.
        (b) Any High scan vulnerabilities must be remediated within 30 days.
        (c) Any Moderate scan vulnerabilities must be remediated within 90 days.
    (2) For all other assets
        (a) Any Critical (Very High) and High scan vulnerabilities must be remediated within 30 days.
        (b) Any Moderate scan vulnerabilities must be remediated within 90 days.

7. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (A&A Package) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk"* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), System Owner, Information System Security Manager (ISSM), and Information System Security Officer (ISSO) will render an authorization decision to:

    - Authorize system operation w/out any restrictions or limitations on its operation;

- Authorize system operation w/restriction or limitation on its operation, or;
- Not authorize for operation.

2. The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. At its option, the Government may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review.

2.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the external system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Vendor deliverables as identified below will be reviewed and accepted or rejected by the process described in GSA CIO IT Security Procedural Guide 19-101, "*External Information System Monitoring*."

Deliverables to be provided Quarterly to the GSA ISSO, ISSM, and/or COR

1. Vulnerability Scanning
   Reference: NIST 800-53 control RA-5
   Provide the most recent Web Application and Operating System vulnerability scan reports. GSA's control parameter for RA-5, Vulnerability Scanning, specifies the following type and frequency of scans; weekly authenticated scans of operating systems (OS)-including databases, monthly unauthenticated scans of web applications, annual authenticated scans of web applications

2. Plan of Action & Milestones (POA&M) Update
   Reference: NIST 800-53 control CA-5
   Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided Annually or when there is a major change to the GSA ISSO, ISSM, and/or COR

Note: Deliverables annotated with a "*" below may be attested to via an attestation letter as described in GSA CIO-IT Security-19-101, "*External Information System Monitoring.*"

1. Updated A&A documentation including the System Security Plan, Contingency Plan, and Business Impact Analysis

    a. System Security Plan
    Reference: NIST 800-53 control PL-2
    Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*

    b. Contingency Plan
    Reference: NIST 800-53 control CP-2
    Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide for Federal Information Systems"*, and GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*

    c. Business Impact Analysis
    Reference: NIST 800-53 control CP-2
    Provide an annual update to the business impact analysis completed in accordance with NIST 800-34, *"Contingency Planning Guide for Federal Information Systems"*, and GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*

2. User Certification/Authorization Review Documents
    Reference: NIST 800-53 control AC-2
    Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

3. *Separation of Duties Document/Matrix
    Reference: NIST 800-53 control AC-5
    Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

4. *Information Security Awareness and Training Records
    Reference: NIST 800-53 control AT-4
    Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

5. Annual FISMA Self-Assessment
    Reference: NIST 800-53 control CA-2

Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

6. *System(s) Baseline Configuration Standard Document
   Reference: NIST 800-53 control CM-2/CM-2(1)
   Provide a well-defined, documented, and up-to-date specification to which the information system is built.

7. System Configuration Settings Verification
   Reference: NIST 800-53 control CM-6/CM-6(1)
   Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening systems, as reviewed and accepted by the GSA AO.

   Provide the most recent operating system Configuration Settings Compliance scan report.

8. Configuration Management Plan
   Reference: NIST 800-53 control CM-9
   Provide an annual update to the Configuration Management Plan for the information system.

9. Contingency Plan Test Report
   Reference: NIST 800-53 control CP-4
   Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

10. Incident Response Test Report
    Reference: NIST 800-53 control IR-3
    Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

11. Information System Interconnection Security Agreements (if applicable)
    Reference: NIST 800-53 control CA-3
    Provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* if there are existing or

new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

12. *Rules of Behavior
    Reference: NIST 800-53 control PL-4
    Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

13. Penetration Testing Report
    Reference: NIST 800-53 control CA-8
    All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

14. *Personnel Screening and Security
    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"* and GSA Order ADM 2181.1, "*Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors."* GSA separates the risk levels for personnel working on Federal computer systems as follows:

    - A favorable initial fitness/suitability determination must be granted and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.
    - A favorable initial fitness/suitability determination must be granted and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.
    - A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested in order to maintain GSA business operations; however such requests should be used judiciously and not incur unnecessary risks to GSA.

If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

Deliverables to be provided Biennially to the GSA ISSO, ISSM, and/or COR

Note: Deliverables annotated with a "*" below may be attested to via an attestation letter as described in GSA CIO IT Security Procedural Guide 19-101, "*External Information System Monitoring.*"

1. Policies and Procedures
   Develop and maintain current the following policies and procedures:
   a. *Access Control Policy and Procedures (NIST 800-53 AC-1)
   b. *Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
   c. *Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
   d. *Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
   e. *Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
   f. *System Maintenance Policy and Procedures (NIST 800-53 MA-1)
   g. *Media Protection Policy and Procedures (NIST 800-53 MP-1)
   h. *Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
   i. *Personnel Security Policy and Procedures (NIST 800-53 PS-1)
   j. *System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
   k. *System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
   l. *Key Management Policy (NIST 800-53 SC-12)

2.6 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall work with GSA to prepare a Privacy Threshold Assessment (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with a privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of GSA's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. Instructions for the PTA and PIA forms can be found at GSA's PIA webpage.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Per OMB A-130 Privacy Act Statements must include:

(1) the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
(2) the principal purpose(s) for which the information is intended to be used;
(3) the published routine uses to which the information is subject;
(4) the effects on the individual, if any, of not providing all or any part of the requested information; and
(5) an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

An example Privacy Act Statement is available at GSA's Privacy Act Statement for Design Research.

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's mandatory privacy awareness and role-based training courses. This includes contractors who work with PII as part of their work duties (e.g., Human Resource staff, Finance staff, and managers/supervisors).

2.7 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from GSA technical guidelines, NIST guidelines,

Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the GSA AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and do not alter the benchmark settings.

3. The Contractor shall cooperate in good faith in defining non-disclosure agreements (NDAs) that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration

shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

6. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system , unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

3 Internal Information Systems - IT Security and Privacy Requirements

3.1 Required Policies and Regulations for GSA Contracts

Federal Laws, Regulations, and Guidance:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "*Responsibilities for Federal Information Systems Standards*"
- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- HSPD 12, "*Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*"
- OMB Circular A-130, "*Managing Information as a Strategic Resource*"
- OMB M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)*"
- OMB M 14-03, "*Enhancing the Security of Federal Information and Information Systems*"
- OMB M-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications*"

- OMB M-15-13, "*Policy to Require Secure Connections across Federal Websites and Web Services*"
- OMB M-17-12, "*Preparing for and Responding to a Breach of Personally Identifiable Information*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*"
- FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"
- NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*"
- NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-53A, Revision 4, *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*"
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-122, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.3, "*Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2200.1, "*GSA Privacy Act Program*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

The contractor shall comply with the following GSA policies listed below when inside a GSA building or inside a GSA firewall.

- GSA Order CIO 2100.3, "*Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities*"
- GSA Order ADM 9732.1, "*Personnel Security and Suitability Program Handbook*"

The GSA policies listed in this paragraph must be followed, if applicable.

- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2104.1, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, "*Mandatory Use of Personal Identity Verification (PIV) Credentials*"

GSA Procedural Guides:

GSA IT Procedural Guides are guidance, unless required by a GSA Directive/Policy, in which case usage is mandatory.

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with GSA Office of the Chief Information Security Officer to determine if it can be made available.

3.2 GSA Security Compliance Requirements

FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems,"* is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Information systems supporting GSA must meet the minimum security and privacy requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 4 (hereafter described as NIST 800-53), *"Security and Privacy Controls for Federal Information Systems and Organizations."*

To comply with the federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* and then the contractor shall apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are available in the GSA Control Tailoring Workbook referenced in Appendix A of this document.

The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems. Where a GSA security hardening benchmark exists, it must be used. GSA security hardening benchmarks may be exceeded but not lowered. GSA benchmarks are available on the GSA Intranet and will be provided by GSA upon request.

3.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The following table identifies essential security controls from the respective baselines to highlight their importance; ensure they are implemented; and identify integration requirements with GSA's IT and IT Security environment. Systems shall have these essential security controls implemented. Further, the proposed system and security architecture of the information system shall be reviewed and approved by the Security Engineering Division, in the Office of the Chief Information Security Officer before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance
AC-2	Account Management	L, M, H	Account management systems must leverage or integrate seamlessly with an existing GSA Access and Identity Management Solution such as GAMS, PIV-based authentication, or other GSA-supported Single-Sign-On solution.
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses to the internal information system must be routed through GSA's managed network access control points, subjecting them to security monitoring.
AU-2	Audit Events	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable GSA IT Security Technical Hardening Guides (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log. For technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security (CIS) benchmark, recommended by the GSA S/SO or Contractor to be approved by the GSA AO shall be used. Internal Information systems shall transmit OS audit log events to GSA's Enterprise Logging Platform (ELP) when possible. OS audit logs not able to be transmitted to the ELP, web application, database, and other logs will be retained by the system owner.

Control ID	Control Title	Baseline	GSA Implementation Guidance
AU-6 (1)	Audit Review, Analysis, and Reporting	M, H	Internal systems must integrate with GSA's Security Stack as specified in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk,"* which supports review of OS audit log events via GSA's Enterprise Logging Platform (ELP). OS audit logs not able to be transmitted to the ELP, web application, database, and other logs will be reviewed by the system owner.
CM-6	Configuration Settings	L, M, H	Information systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as reviewed and accepted by the GSA AO. Further, all workstations and servers connected to the GSA network shall have BigFix and have agents installed.
CM-7	Least Functionality	L, M, H	Internal systems must integrate with GSA's Security Stack as specified in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk*," which supports least functionality via GSA's implementation of Bit9.
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Cloud Infrastructure as a Service (IaaS) architectures shall implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecom Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H	All information systems shall implement multi-factor authentication for privileged accounts. Information systems shall technically integrate with a GSA supported enterprise identification and authentication solution (e.g., SAML 2.0 with SSO integration (following 2FA with HSPD-12 PIV card)).

Control ID	Control Title	Baseline	GSA Implementation Guidance
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	L, M, H	All information systems must implement multi-factor authentication for non-privileged accounts. Information systems shall technically integrate with a GSA supported enterprise identification and authentication solution (e.g., SAML 2.0 with SSO integration (following 2FA with HSPD-12 PIV card)).
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: Cryptographic Module Validation Program Validated Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.
PL-8	Information Security Architecture	M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.
RA-5	Vulnerability Scanning	L, M, H	All systems must integrate with the GSA vulnerability scanning tool set managed by the Security Operations Division in the Office of the Chief Information Security Officer. Information systems shall coordinate integration with the scanning program by contacting SecOps@gsa.gov.
SA-22	Unsupported System Components	GSA Required	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on GSA's Enterprise Architecture IT Standards List.

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-8/ SC-8(1)	Transmission Confidentiality and Integration	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption. Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains. (see Binding Operational Directive (BOD) 18-01, Enhance Email and Web Security). SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."*
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms
SC-17	PKI Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69*, "SSL/TLS Implementation,"* and NIST Special Publications 800-32and 800-63.
SC-18	Mobile Code	M, H	Systems must adhere to GSA's requirements regarding IT Standards and CIO-IT Security-07-35, "*Web Application Security*" and CIO-IT Security-17-81, "*Web Browser Technologies Hardening*," as applicable, to ensure only approved code (including mobile code) is used.
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	L, M, H	**Systems that process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Authenticators (e.g., passwords, tokens, keys, certificates, hashes, etc.), and other sensitive data as determined by the AO, shall encrypt that data everywhere (i.e., at file level, database level, at rest, and in transit (see SC-8(1)). For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption or tokenization is also acceptable. For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption.** Encryption algorithms shall be FIPS-approved with FIPS-validated encryption modules.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, critical/very high vulnerabilities for Internet-accessible IP addresses must be remediated within 15 days, for all other assets critical/very high vulnerabilities must be remediated within 30 days; High vulnerabilities must be remediated within 30 days; Moderate vulnerabilities must be remediated within 90 days.
SI-3	Malicious Code Protection	L, M, H	All internal information systems must incorporate Bit9 and FireEye HX agents on supported operating systems. These agents will be provided.
SI-4	Information System Monitoring	L, M, H	All information systems must be monitored internally and across ingress/egress points for potentially malicious activity. In addition, all internal information systems must incorporate Bit9 and FireEye HX agents on supported operating systems. These agents will be provided.
SI-10	Information Input Validation	M, H	All system accepting input from end users must validate the input in accordance to industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security,"* and OWASP Top 10 Web Application Security Vulnerabilities.

Control ID	Control Title	Baseline	GSA Implementation Guidance
AR-2	Privacy Impact and Risk Assessment	See note below	The contractor shall conduct a Privacy Threshold Assessment (PTA) and, if applicable, a Privacy Impact Assessment (PIA) identifying the categories of information and addressing potential risks to PII. The contractor also shall coordinate with the GSA Privacy Office concerning these documents.
AR-8	Accounting of Disclosures	See note below	The contractor shall keep an accurate accounting of disclosures of information held in any system of records under its control.
TR-2	System of Records Notices and Privacy Act Statements	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure System of Records Notices (SORNs) and Privacy Act notices on forms that collect Personally Identifiable Information (PII) are established and kept current.
UL-1	Internal Use	See note below	The contractor shall ensure that PII is shared internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
UL-2	Information Sharing with Third Parties	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure PII is shared in accordance with GSA requirements and agreements with third parties.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

3.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 2 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk,"* provide guidelines for performing the A&A process. The system/application must have a valid assessment and authorization, known as an Authorization to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) when significant changes are made to the system, and as specified in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk,*" and the guides for GSA's other A&A processes referenced therein.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing

Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following A&A documentation:

- System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems,*" and completed in accordance with GSA SSP requirements and templates. The SSP shall include as appendices required policies and procedures across 17 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Security Agreements (in agreement with NIST Special Publication 800-47, *"Security Guide for Interconnecting Information Technology Systems"*). The SSP shall include; as an appendix, a completed GSA Control Tailoring Workbook (CTW) identified in Appendix A of this guide. The column in the CTW titled "Vendor/Contractor Defined Values" shall be used to document all contractor implemented parameter settings that differ from the GSA Defined Value and the Vendor/Contractor defined value when the value is deferred to the Vendor/Contractor. GSA's approval will be documented in the CTW column titled "GSA Approval of Vendor/Contractor Defined Values."
- Contingency Plan completed in agreement with NIST Special Publication 800-34 and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
- Business Impact Analysis completed in agreement with NIST Special Publication 800-34 and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
- Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning.*"
- Plan of Action & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)*."
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all Internet accessible, all FIPS 199 High, and all High Value Asset (HVA) information systems. These systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37 Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,*" and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk*" or via continuous monitoring based on GSA IT Security Procedural Guide 12-66, "*Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program*" that is reviewed and accepted by the GSA CISO.

3. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk*."
4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk*." Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.
5. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."* Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.
6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. Vulnerabilities must be mitigated as follows:
    (1) For Internet-accessible IP addresses
        (a) Any Critical (Very High) scan vulnerabilities must be remediated within 15 days.
        (b) Any High scan vulnerabilities must be remediated within 30 days.
        (c) Any Moderate scan vulnerabilities must be remediated within 90 days.
    (2) For all other assets
        (a) Any Critical (Very High) and High scan vulnerabilities must be remediated within 30 days.
        (b) Any Moderate scan vulnerabilities must be remediated within 90 days.
7. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (A&A Package) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), System Owner, Information System Security Manager (ISSM), and Information System Security Officer (ISSO)) will render an authorization decision to:
    - Authorize system operation w/out any restrictions or limitations on its operation;
    - Authorize system operation w/ restriction or limitation on its operation, or

- Not authorize for operation.

2. The System Owner, AO, and supporting stakeholders including but not limited to System Custodians, supporting contractors, etc., shall make appropriate personnel available for interviews and provide documentation to the Federal Government, or their designee acting as their agent, in order to verify compliance with the requirements of GSA's Information Technology security program.

3.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractors system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided Quarterly to the GSA ISSO, ISSM, and/or COR

1. Plan of Action & Milestones (POA&M) Update
   Reference: NIST 800-53 control CA-5
   Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided Annually or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Updated A&A documentation including the System Security Plan, Contingency Plan. and Business Impact Analysis

   a. System Security Plan
      Reference: NIST 800-53 control PL-2
      Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*
   b. Contingency Plan
      Reference: NIST 800-53 control CP-2
      Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide for Federal Information Systems"* and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
   c. Business Impact Analysis
      Reference: NIST 800-53 control CP-2

Provide an annual update to the business impact analysis completed in accordance with NIST 800-34, *"Contingency Planning Guide for Federal Information Systems"*, and GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*

2. User Certification/Authorization Review Documents
   Reference: NIST 800-53 control AC-2
   Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

3. Annual FISMA Self-Assessment
   Reference: NIST 800-53 control CA-2
   Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

4. System Configuration Settings
   Reference: NIST 800-53 control CM-6
   Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as reviewed and accepted by the GSA AO.

   All workstations and servers connected to the GSA network integrate with BigFix and have agents installed. Provide the most recent operating system Configuration Settings Compliance scan report.

5. Configuration Management Plan
   Reference: NIST 800-53 control CM-9
   Provide an annual update to the Configuration Management Plan for the information system.

6. Contingency Plan Test Report
   Reference: NIST 800-53 control CP-4
   Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed

once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

7. Incident Response Test Report
   Reference: NIST 800-53 control IR-3
   Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response*."

8. Information System Interconnection Security Agreements (if applicable)
   Reference: NIST 800-53 control CA-3
   Systems with interconnections shall provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

9. Penetration Testing Report
   Reference: NIST 800-53 control CA-8
   All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

10. Personnel Screening and Security
    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA Order ADM 2181.1, "*Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors."* GSA separates the risk levels for personnel working on Federal computer systems as follows:

    - A favorable initial fitness/suitability determination must be granted and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.
    - A favorable initial fitness/suitability determination must be granted and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the

System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.

- A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested in order to maintain GSA business operations; however such requests should be used judiciously and not incur unnecessary risks to GSA.

If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

3.6 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall work with GSA to prepare a Privacy Threshold Assessment (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with a privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of GSA's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. Instructions for the PTA and PIA forms can be found at GSA's PIA webpage.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Per OMB A-130 Privacy Act Statements must include:

(1) the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
(2) the principal purpose(s) for which the information is intended to be used;
(3) the published routine uses to which the information is subject;
(4) the effects on the individual, if any, of not providing all or any part of the requested information; and
(5) an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

An example Privacy Act Statement is available at GSA's Privacy Act Statement for Design Research.

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's mandatory privacy awareness and role-based training courses. This includes contractors who work with PII as part of their work duties (e.g., Human Resource staff, Finance staff, and managers/supervisors).

3.7 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the GSA AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and do not alter the benchmark settings.
3. The Contractor shall cooperate in good faith in defining non-disclosure agreements (NDAs) that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to facilities, installations, technical capabilities, operations, documentation, records, and databases used to provide or facilitate services for the Government within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans.
        - Authenticated and unauthenticated web application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

    b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

6. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system , unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

4 Low Impact Software as a Service (LiSaaS) – IT Security and Privacy Requirements

To be considered for award, the contractor must comply with GSA IT's Low-Impact SaaS (LiSaaS) review. The successful vendor will need to ensure any software-as-a-service provided under this contract meets GSA security and privacy requirements prior to invoicing the government for services received under this contract. This includes working with GSA to ensure the Software-as-a-Service (SaaS) passes the current Low-impact-software-as-a-service (LiSaaS) approval process, as outlined in GSA IT Security Procedural Guide 16-75, "*Low Impact Software as a Service (SaaS) Solutions Authorization Process*."

4.1 Assessment of the System

The contractor shall provide evidence in support of meeting the requirements for the review activities stated in GSA IT Security Procedural Guide 16-75, "*Low Impact Software as a Service (SaaS) Solutions Authorization Process*," and as summarized below. As stated in the guide items (2)-(6) in the list below, may be satisfied by a letter of attestation submitted by the Office of the Chief Security Officer ISSO Support Division (IST) Director or designee, based on a demonstration and review of artifacts. A checklist template will be provided to the contractor, as applicable.

(1) Completion of a LiSaaS Solution Review Checklist Template (including supporting artifacts). This checklist provides a summary of the service function and purpose provided by the LiSaaS solution. It includes the who, what, when, where, and how of the solution, including any leveraged infrastructures and SaaS integrations, as applicable. Instructions are contained in the template. In the process of completing the checklist solutions deemed to be very low/negligible risk will have a LiSaaS Solutions Profile completed by GSA support personnel.

(2) Document how system and security parameters deferred to customers are implemented.
(3) Submit latest web application scan results (e.g., NetSparker, Acunetix, Burp Suite Pro, etc.). The OCISO can assist with web application scans if vendor(s) do not have an in house web application scanning capability.
(4) Submit latest operating system (OS) vulnerability scan results (e.g., Tenable Nessus, Qualys, nCircle, McAfee Vulnerability Manager, etc.). Reference NIST SP 800-53 control RA-5 - Vulnerability Scanning.
    a. Vendors that are Payment Card Industry Data Security Standard (PCI DSS) compliant or have the McAfee Secure Seal or TrustGuard Seal may provide the results of their latest PCI DSS Compliant, McAfee Secure Seal or TrustGuard quarterly scan.
    b. Vendors that do not meet the PCI DSS, McAfee, or TrustGuard standards listed, must provide their most recent OS vulnerability scan results.
(5) An acceptable flaw remediation process. Vendors must be able to identify and remediate information system flaws in a timely manner.
(6) Results of one of the following audits/certifications:
    - Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 18
    - SysTrust/WebTrust
    - ISO/IEC 27001
    - Payment Card Industry Data Security Standard (PCI DSS)

Note: Although the minimum requirement is for the SSAE/SOC 2 audit report or one of the vendor certifications; the GSA AO and the CISO will take a holistic view of the application based on all of the documentation presented to determine the overall risk of the application as well as any residual risks that may need to be accepted when considering the application for use. If the documentation presented does not provide an adequate understanding of the systems security posture and/or is deemed insufficient to make a risk determination; additional information will be required.

4.2 Authorization of the System

The authorization process supports an ATO valid for:

- No more than one year if the application is determined to be Low Risk based on the evidence provided.
- Up to three years if the application is determined to be a commodity ancillary service that presents Very Low/Negligible Risk based on the evidence provided.

If not already FedRAMP authorized, any application granted a one year ATO must obtain a FedRAMP tailored authorization within one year of its ATO. If, within three months of receiving its one year ATO, progress towards a FedRAMP Tailored authorization has not been observed, GSA will start to cease engagement with the vendor and pursue alternative solutions. For

detailed requirements of a FEDRAMP Tailored authorization visit the FEDRAMP Tailored for Low-Impact Software-as-a-Service (LI-SaaS) page. Without a LiSaaS approval, GSA will not be able to use the software for the base year of the contract, and without FedRAMP approval, GSA will be unable to use the product for the option years of the contract.

The contractor's agreement to the LiSaaS and FedRAMP requirements are required. If the contractor does not agree, no contract award will be made.

If at any time, the vendor is either unwilling or unable to meet any of the process requirements, GSA may choose to cancel the contract and terminate any outstanding orders.

4.3 Maintenance of ATO and Continuous Monitoring

The LiSaaS ATO will be contingent on annual validation of the requirements identified in Section 4.1, including:

- The latest SSAE/SOC 2 audit report, vendor certification, or PCI DSS compliance;
- Annual web application vulnerability scan results;
- Most recent quarterly operating system vulnerability scan results or proof of compliance with PCI DSS, McAfee Secure Seal, or TrustGuard standards/seals;
- Annual recertification that GSA is still using the service.

Note: If an attestation letter was used to validate any of the requirements listed above for the existing ATO, then a new attestation letter or the artifact/deliverables listed must be provided.

If at any time, the vendor is either unwilling or unable to meet any of the requirements, the ATO shall be terminated upon approval of the AO. It is the responsibility of the assigned ISSO to ensure the requirements continue to be met. Significant changes shall be reported to the ISSM, who with the ISSO manages the A&A package.

The vendor shall report if its audit report/certification renews or expires and if any of the other required activities cannot be supported.

4.4 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, disclosed, or developed as a result of work under this contract. The contractor shall also protect all Government data, etc. by treating the information as sensitive. All information gathered or created under this contract should be considered as confidential information. It is anticipated that this information will be gathered, created and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information. Personnel shall adhere to the Privacy Act, Title 5 of the U. S. Code, Section 552a and applicable agency rules and regulations.

4.5 Data Ownership and Unrestricted Rights to Data

All Government data collected in the system is the property of the Federal Government. The Government will retain unrestricted rights to government data. The ordering activity retains All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

Government data rights of software deliverables shall be in accordance with FAR 52. 227-19 Commercial Computer Software License and/or FAR 52. 227-14 Rights in Data - General. Ownership of data entered into any and all systems, system documentation, all deliverables produced in the performance of this contract, and other related system information shall reside with the Government.

The Contractor shall place the following copyright notice on all materials, documents, deliverables, etc. developed during the performance of this contract:

For purposes of clarity, the intent of the government is for intellectual property to be vested in the federal government for work paid for by the federal government. All documents, graphics, and code created under this contract are the intellectual property of the federal government including, but not limited to, plans, reports, schedules, software code, software designs, graphics, etc. In the event that the federal government implements under this contract open-source software and pays for the cost of the implementation of open-source software, the final changes and edits to the code and configuration (such as work to integrate plug-ins) are the intellectual property of the federal government.

4.6 Personally Identifiable Information

Personally identifiable information (PII) data **is not** in the scope of the acquisition and PII data **is not** expected to be stored in the vendor's SaaS solution. The contractor shall work with GSA to prepare a Privacy Threshold Assessment (PTA) to either document PII is not in scope, or determine which categories of information will be stored, processed, or transmitted by the system. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

Privacy data (should it come into scope) will require that the vendor’s SaaS solution be FedRAMP authorized at least at the FIPS PUB 199 Moderate level.

4.7 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

4.8 Data Release

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the SaaS solution or to provide the SaaS solution to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

4.9 Confidentiality and Nondisclosure

Personnel (contractor/subcontractor employee)working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements (NDA/CUI) to guarantee the protection and integrity of Government information and documents. The Contractor shall submit to the COR a completed confidentiality and NDA form for each individual contractor/subcontractor.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U. S. C. §§ 1030.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request GSA OGC can advise on NDA development.

4.10 Section 508 Compliance

The Contractor(s) shall provide accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U. S. C. 794d). All electronic and information technology (EIT) delivered must meet the applicable accessibility standards at 36 CFR 1194, unless an agency exception to this requirement exists. The 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended. All deliverables will be Section 508 compliant, and will be reviewed for compliance by the government which reserves the right to reject the deliverable(s) until remediation of deficiencies has been successfully completed by the Contractor. Complete technical descriptions are provided on the following website: http://www.section508.gov.

Where appropriate, the Contractor(s) shall indicate whether each product or service is

compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the quote must indicate where full details of compliance can be found (e. g., vendor's website or other exact location).

4.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*."
2. The contractor shall cooperate in good faith in defining NDAs that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request GSA OGC can advise on NDA development.

3. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.
    b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e. g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
    c. The program of inspection shall include, but is not limited to:
        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration

shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

d. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

4. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

5. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system , unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

4.12 Terms of Service

Many terms found in commercial ToS or End User License Agreements (EULA) are not acceptable when the Government is the end user. Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

The Contractor's SaaS will undergo a formal review by GSA as part of the review/approval process. The Contractor's ToS shall be found to be acceptable to the government or a modified ToS negotiated as part of the approval review, prior to final authorization.

4.13 References

GSA IT Security Procedural Guide 16-75, "*Security Reviews for Low Impact Software as a Service (SaaS) Solutions Authorization Process*"

FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems"*

Guide to Understanding FedRAMP

5 Cloud Information Systems – IT Security and Privacy Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for **<SELECT Low, Moderate, or High>** impact systems (as defined in FIPS PUB 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for **<SELECT Low, Moderate, or High>** impact systems. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"* (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

GSA may choose to cancel the contract and terminate any outstanding orders if the contractor has its FedRAMP authorization (Joint Authorization Board [JAB] Provisional or Agency) revoked and the deficiencies are greater than agency risk tolerance thresholds.

5.1 Assessment and Authorization

5.2 Assessment of the System

1. The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's FIPS PUB 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at FedRAMP.

    - Privacy Impact Assessment (PIA)
    - FedRAMP Test Procedures and Results
    - Security Assessment Report (SAR)
    - System Security Plan (SSP)
    - Contingency Plan (CP)
    - Business Impact Analysis
    - Contingency Plan (CP) Test Results
    - Plan of Action and Milestones (POA&M)
    - Continuous Monitoring Plan (CMP)
    - FedRAMP Control Tailoring Workbook
    - Control Implementation Summary Table
    - Results of Penetration Testing
    - Software Code Review

- Interconnection Security Agreements/Service Level Agreements/Memorandum of Agreements

2. Information systems must be assessed by an accredited FedRAMP Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
3. The Government reserves the right to perform Security Assessment and Penetration Testing (of its instance). If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment and Penetration Testing activities to include control reviews in accordance with FedRAMP requirements. Penetration shall be supported by mutually agreed upon Rules of Engagement (RoE). Review activities include but are not limited to manual penetration testing; automated scanning of operating systems, web applications; wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
4. The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct on-site inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.
5. Physical Access Considerations – If the Cloud Service Provider (CSP) is operated within an Infrastructure as a Service (IaaS) that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
6. Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before a GSA authorization is issued.
7. The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

5.3 Authorization of the System

1. If the CSP Software as a Service (SaaS) or Platform as a Service (PaaS) is FedRAMP authorized (i.e., listed as FedRAMP authorized on the FedRAMP website:

   https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=Compliant

   GSA will leverage the CSP's FedRAMP Assessment and Authorization package to document and assess the customer controls for which GSA has responsibility and issue a GSA ATO for the agency's instance of the CSP's SaaS or PaaS offering. The CSP shall work with the GSA to facilitate documentation and assessment of required customer controls, as necessary.

2. If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized, it shall:

   a. Operate on an CSP IaaS environment that is FedRAMP authorized; AND

   b. Be listed as FedRAMP In Process on the FedRAMP Website - https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=In%20Process

      OR be listed as FedRAMP Ready on the FedRAMP website - https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=FedRAMP%20Ready

   c. Shall deliver within 90 days of contract award a FedRAMP Readiness Assessment Review completed by a FedRAMP 3PAO following the FedRAMP Readiness Assessment Guidelines. The FedRAMP Readiness Assessment Review demonstrates the CSPs overall readiness for FedRAMP authorization and whether it has a viable path to achieve a FedRAMP authorization within one (1) year of the contract award. If the CSP does not provide a FedRAMP Readiness Assessment as prescribed or the assessment demonstrates a significant gap in capabilities that will preclude achievement of a FedRAMP authorization within 1 year of the contract award, then, GSA will terminate the contract.

   If requirements a-c, as defined above, are met the CSP will have one (1) year from the date of contract award to achieve FedRAMP authorization. During this transitional period, GSA may issue an agency specific authorization (i.e., not FedRAMP) not to exceed one (1) year (to allow the CSP to achieve FedRAMP compliance) leveraging an existing ATO with another Federal Department/Agency (D/A) (with supporting A&A Package). The CSP may have a non-FedRAMP ATO with another D/A or be based on the GSA Moderate Impact SaaS Solutions process as described in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk."* The CSP shall make available any existing assessment and authorization package for GSA review and provide necessary documentation and access to facilitate the GSA Moderate Impact SaaS A&A process. Without a FedRAMP authorization within 1 year of contract award; GSA will not be able to use the product for the option years and shall terminate the contract.

3. CSP shall ensure these essential security controls are implemented. CSP shall implement FedRAMP control parameters and implementation guidance, as applicable. Further, the CSP shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code (as applicable)) and/or the start as A&A activities.

Control ID	Control Title	FedRAMP Baseline
AC-2	Account Management	L, M, H
AU-2	Audit Events	L, M, H
CM-6	Configuration Settings	L, M, H
CP-7	Alternative Processing Site	M, H
CP-8	Telecom Services	M, H
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H
IA-2 (12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	L, M, H
IA-7	Cryptographic Module Authentication	L, M, H
MP-4	Media Storage	M, H
MP-5	Media Transport	M, H
PL-8	Information Security Architecture	M, H
RA-5	Vulnerability Scanning	L, M, H
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H
SC-13	Cryptographic Protection	L, M, H
SC-17	PKI Certificates	M, H
SC-18	Mobile Code	M, H
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H

Control ID	Control Title	FedRAMP Baseline
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	M, H
SI-2	Flaw Remediation	L, M, H
SI-3	Malicious Code Protection	L, M, H
SI-4	Information System Monitoring	L, M, H
SI-10	Information Input Validation	M, H

5.4 Reporting and Continuous Monitoring

Maintenance of the FedRAMP Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated in agreement with FedRAMP guidelines and submitted to the MAX.Gov Portal or repository designated by the FedRAMP program.

The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the Federal Departments/Agencies leveraging the services providers' cloud offering to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

The contractor shall provide continuous monitoring deliverables in support of a one (1) year conditional authorization (if necessary) to achieve FedRAMP authorization. Deliverables shall include:

- Quarterly OS-including database, and web application, vulnerability scans as specified in the NIST SP 800-53 Control RA-5 parameter in GSA's Control Tailoring Workbook (deliverable shall include raw results and findings shall be included in the POA&M document);
- Quarterly Plan of Action and Milestones (POA&M);
- Annual A&A Package updates including the System Security Plan, Contingency Plan, Business Impact Analysis, Configuration Management Plan, Contingency Plan Test Report, and Annual FISMA Assessment.

Upon achievement of FedRAMP authorization, GSA will accept the FedRAMP A&A and continuous monitoring documentation made available on the MAX.Gov Portal or a repository

designated by the FedRAMP program in agreement with FedRAMP guidelines to satisfy the continuous monitoring requirement.

5.5 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy,"* and GSA Order ADM 2181.1, "*Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors."* GSA separates the risk levels for personnel working on Federal computer systems as follows:

- A favorable initial fitness/suitability determination must be granted and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.
- A favorable initial fitness/suitability determination must be granted and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.
- A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested in order to maintain GSA business operations; however such requests should be used judiciously and not incur unnecessary risks to GSA.

If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

5.6 Sensitive Information Storage

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no

longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, *"Guidelines for Media Sanitization."* The destruction, purging or clearing of media specific to the CSP will be recorded and supplied upon request of the Government.

5.7 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this contract should be considered as SBU information. If contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same FedRAMP requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

5.7.1 Unrestricted Rights to Data

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

5.7.2 Personally Identifiable Information

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of acquisition and PII **<SELECT: is or is not>** expected to be stored in the vendor's cloud solution. The vendor shall prepare a Privacy Threshold Assessment (PTA) to either document PII is not in scope, or determine which categories of information will be stored, processed, or transmitted by the system. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not

providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

5.7.3 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

5.7.4 Data Release

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

5.8 Data Ownership

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

5.9 Confidentiality and Nondisclosure

Personnel working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

5.10 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee NDA. The Contractor shall submit to the COR a completed confidentiality and NDA for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this NDA, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

5.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be

used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*

2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the GSA AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and do not alter the benchmark settings.

3. The contractor shall cooperate in good faith in defining NDA that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

4. The contractor shall comply with any additional FedRAMP privacy requirements.

5. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

    b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

    c. The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

d. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

6. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

7. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system , unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

5.12 References

Guide to Understanding FedRAMP

FedRAMP Cloud Computing Documents

FedRAMP Templates

6 Mobile Application - IT Security and Privacy Requirements

The contractor shall generally, substantially, and in good faith follow GSA IT Security Policy and Guidelines including GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,*" or current versions. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

6.1 General Mobile Application Guidelines

1. The Mobile Application (App) shall be integrated with a Mobile Device Management (MDM) solution. GSA currently uses MAAS 360.
2. The contractor shall provide to the GSA IT Contracting Officer Representative (COR) the source code and all supporting artifacts of the app for security testing via the GSA Static and mobile Code Scanning program. In addition, the contractor shall actively participate in the program to remediate all findings according to the most recent Static Code Scanning Standard Operating Procedure (SOP) before the beta and production App is accepted by GSA. Once the contract is awarded, GSA will provide a copy of the Static Code Scanning SOP to the contractor.
3. The contractor shall provide clear and concise documentation so that future developers and programmers can understand the processes used and are able to enhance, edit or build upon the original App. All source code information prepared for this App is the property of GSA, Federal Acquisition Service, OCCM and GSA IT.
    - The contractor shall provide detailed process and code documentation.
    - The contractor shall provide App features documentation.
    - The contractor shall support development and updates of a security authorization package for the App following the process requirements documented in GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,"* or current version.

6.2 Mobile Device Security

The contractor shall adhere to the following requirements and guidelines for developing mobile applications. All requirements and guidelines are found in the GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,"* which will be provided upon contract award.

A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user's PC. However, as mobile

app development has grown, a more sophisticated approach involves developing applications specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you do not have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, GSA will concentrate security focus on the following goals:

- That all apps loaded have an initial assessment by GSA for acceptability and then a security assessment & authorization, when required
- That all apps are deployed from only trusted sources, following their security/assessment process – This presently is the Apple ITunes store for iOS and the Google Play store for Android. MaaS360 may also be used, once retrieved from these sources, for enterprise deployment
- That Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for GSA as an Agency
- That apps deemed to be unacceptable are blacklisted, using MaaS360
- That a mobile app inventory for all devices be maintained
- That GSA developed apps are assessed, evaluated and approved by the AO for the system they support before deployment

6.3 Application Sources

Allowing mobile apps to be loaded from an unknown source presents one of the greatest risks to GSA's environment when using mobile devices. "Side loading" of apps is a process where a user installs an application from a source other than the Apple ITunes store or Google Play store. If a user jailbreaks a device, side loading can occur as well. Jailbreaking, or rooting, is a process where an Operating System (OS) of a mobile device grants a user or application root level access to the OS. While iOS devices that are not jailbroken/rooted protect against sideloading, the Android OS allows a user to turn such protection on/off (allow unknown sources) if not managed by MDM.

As such, the following policies apply to all GSA devices (Government and Bring Your Own Device) used in the environment to protect against side loading of apps:

- Devices shall not be jailbroken/rooted by users or apps loaded by users. GSA's MDM solution shall immediately notify an administrator of all such incidents immediately for remediation.
- Unknown sources shall not be enabled by users or applications. GSA's MDM solution shall immediately notify an administrator of all such incidents for remediation.
- GSA developed apps may be sideloaded for testing purposes only on test devices, but production deployment of GSA developed apps may only be done via the policies outlined below for Apple iOS and Google Android.

The GSA MaaS store may be employed for enterprise deployments, but only after the app has undergone the review/approval processes outlined below:

- Apple App Review guidelines
- Google Play Store Developer Policy Center

6.4 Terms of Service (ToS)

Many terms found in commercial TOS or End User License Agreements (EULA) are not acceptable when the Government is the end user. Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

Apps deemed to be acceptable are loaded at the discretion of the user for either personal use or as a personal productivity tool to further enhance the work experience. As such, use of the App is not mandated by the agency. Therefore, acceptance of the ToS falls upon the user as an individual. This is true even if the App is loaded using a GSA.gov domain account or registered with a user's GSA.gov email address.

Apps that are approved after formal assessment: and include a formal review by GSA Counsel as part of the review/approval process, where the ToS was found to be acceptable to the government or a modified ToS was negotiated as part of the approval review, prior to final authorization. When loaded and activated, the user is accepting the ToS (often a technical function required of the user), not as an individual, but as an employee or contract employee assigned to perform work functions for GSA.

6.5 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's App. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall work with GSA to prepare a Privacy Threshold Assessment (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the App. The PTA must be completed before development begins and whenever a change with privacy impact (e.g., a new category of information is collected) is made to an existing App. PTAs are required to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the App. Information regarding instructions for the PTA and PIAs can be found at GSA's PIA webpage.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's App must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.

- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Per OMB A-130 Privacy Act Statements must include:

(1) the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
(2) the principal purpose(s) for which the information is intended to be used;
(3) the published routine uses to which the information is subject;
(4) the effects on the individual, if any, of not providing all or any part of the requested information; and
(5) an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

An example Privacy Act Statement is available at GSA's Privacy Act Statement for Design Research.

Note: Apps that access data a user creates must assume a user may include privacy data/PII in the application unless the data creation is restricted to data controlled by the App.

All contractor staff who have significant privacy information responsibilities must complete GSA's mandatory privacy awareness and role-based training courses. This includes contractors who work with PII as part of their work duties (e.g., Human Resource staff, Finance staff, and managers/supervisors).

6.6 GSA App Development, Assessment, Authorization and Deployment

GSA developed apps are designed to take advantage of the concept of Anytime, Any Where, Any Device (A3) to allow GSA users and customers to access GSA data while mobile. As such, as GSA business lines develop apps for use on the iOS and Android environment, these apps must undergo an assessment and authorization process before being deployed. With that in mind, the following guidelines are to be followed:

- A GSA developed app that supports a GSA FISMA system must be documented in the System Security Plan and authorized to operate as part of a current ATO letter from the respective AO before deployment. GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk,"* is to be followed for this process. Any app that is not directly tied to an already existing system authorized to operate must have an

assessment performed and subsequently approved for release by the Chief Information Security Officer (CISO).

- Any mobile app development shall result in a minimum of the release of both an iOS and Android version of the app. This ensures coverage to all users within GSA and the maximum coverage for apps released to the public. Any additional application versions for alternate OS mobile platforms may be developed for such apps, but iOS and Android shall remain as the core base OS' for GSA developed mobile apps for all releases.
- All GSA developed apps must follow the respective application review and publication guidelines for the OS to which they were developed as outlined in Section 8.2 of GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications"* and the release process documented in this section.
- Other than for testing purposes on non-user provisioned mobile devices, side loading of apps in the environment is not authorized.
- The GSA MaaS360 Store is authorized for enterprise deployment of apps to GSA user devices once that app has been assessed, authorized, and published according to the guidelines outlined in this section.
- Mobile code scanning throughout the development cycle is critical, but before release by the Mobile Device Team, a mobile app must be scanned by the Systems Engineering Division (ISE) Team within the OCISO. This scan is a source code scan using the CheckMarx platform. As with all applications in GSA, no High/Critical findings are allowed from these scan results. Moderate findings should be documented in the respective POA&M for the system by which the app is authorized and accepted by the AO; Low and Informational findings should be taken into consideration by the developers for their next iteration of app development. A detailed process for mobile app release is documented at the end of this section.
- All mobile application development should take into consideration the Open Web Application Security Project (OWASP) Mobile Security Project when developing mobile apps either within GSA or for use by the general public. The guidelines for mobile application security testing from OWASP are linked below:
  - OWASP Mobile Security Testing Guide
  - OWASP Mobile Security Project Home Page
- GSA developed mobile apps must undergo an assessment review and approval process before being released for use. These apps fall into two categories that shall have slightly different processes for approval, with many common steps.
- Mobile apps that are developed as part of another system with a current ATO and provide access to an application using a different form factor (smartphones/tablets), such apps must be documented in the System Security Plan for the system they support.

- Mobile apps designed for a specific purpose not part of a current ATO stand alone in their ATO. As these apps do not have a parent system they support, the below listed process is the complete assessment process required for these apps.

All apps must follow the approval processes outlined below:

1. Apps must be scanned prior to release by the GSA Office of the CISO using the Checkmarx Application scanner. No Critical/High findings may remain for approval to be received and any moderate/medium findings must be contained in a POA&M, either for the system the app is a part of, or a separate POA&M if a standalone mobile app.
2. The privacy requirements as stated above must be met.
3. A mobile application security assessment review in accordance with the GSA-IT Procedural Guide: CIO-IT Security-12-67, "*Securing Mobile Devices and Applications*" must be completed and signed by the mobile App owner, mobile App assessor, mobile App Information System Security Manager (ISSM), a representative of the Office of the CSIO, to denote a proper assessment and review was conducted of the mobile app prior to release.

6.7 Intellectual Property

This task order is funded by the United States Government. All intellectual property generated and/or delivered pursuant to this Firm-Fixed Price Statement of Work will be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with Government funds, a nonexclusive "paid-up" license to practice any patentable invention or discovery made during the performance of this task order, and a "paid-up" nonexclusive and irrevocable worldwide license to reproduce all works (including technical and scientific articles) produced during this task order.

6.8 Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements (NDA/COI) to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

6.9 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee NDA. The Contractor shall submit to the COR a completed confidentiality and NDA form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this NDA, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

Note: GSA's Office of the General Counsel (OFC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

6.10 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA

Order ADM 2181.1, "*Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors."* GSA separates the risk levels for personnel working on Federal computer systems as follows:

- A favorable initial fitness/suitability determination must be granted and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.
- A favorable initial fitness/suitability determination must be granted and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.
- A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested in order to maintain GSA business operations; however such requests should be used judiciously and not incur unnecessary risks to GSA.

If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

6.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security requirements for Cryptographic Modules."*
2. The Contractor shall certify mobile applications are fully functional and operate correctly as intended on mobile devices in accordance with GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications*." The standard installation, operation, maintenance, update, and/or patching of mobile applications shall not alter configuration settings as documented in CIO-IT Security-12-67. Mobile applications

designed for normal end users shall run in the standard user context without elevated administration privileges.

3. The Contractor shall cooperate in good faith in defining NDAs that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

    b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

6. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system , unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

7 Nonfederal Systems and Organizations – IT Security and Privacy Requirements

7.1 Required Policies and Regulations for GSA Contracts

Federal Laws, Regulations, and Guidance:

The contractor shall comply with all applicable Federal Laws, Regulations, and Guidance.

- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- E-Government Act of 2002 section 208, "*44 USC 3501*"
- 32 CFR Part 2002, "*Controlled Unclassified Information*"
- OMB Circular A-108, "*Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*"
- OMB Memo 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"

Federal Standards and Guidance:

The contractor shall comply with the following Federal Information Processing Standards (FIPS) and NIST guidelines.

- FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*"

- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-171, Revision 2, "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*"
- NIST SP 800-171A, "*Assessing Security Requirements for Controlled Unclassified Information*"

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.3, "*Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2200.1, "*GSA Privacy Act Program*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

GSA Procedural Guides:

- GSA IT Procedural Security Guides 01-02, *"Incident Response"*
- GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M)"*
- GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises*"

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with GSA Office of the Chief Information Security Officer to determine if it can be made available.

7.2 GSA Security Compliance Requirements

To comply with the Federal standard, nonfederal systems and organizations shall implement the specific security requirements in NIST SP 800-171, Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" for protecting the confidentiality of Controlled Unclassified Information (CUI). NIST SP 800-171 controls requirements have been tailored for non-federal entities, eliminating requirements, controls, or parts of controls that are uniquely Federal, not directly related to protecting the confidentiality of CUI; or expected to be routinely satisfied by nonfederal organizations without specification. NIST SP 800-171 controls are derived from FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems," and the moderate security control baseline in NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" and are based on the CUI regulation 32 CFR Part 2002, "Controlled Unclassified Information."

The basic and derived security requirements in NIST SP 800-171 provide protection from unauthorized disclosure and unauthorized modification of CUI. The requirements apply only to

the components of non-federal systems that process, store, or transmit CUI, or that provide security protection for such components.

7.3 Security Assessment Activities and Required Documentation

The non-federal system/organization shall implement the NIST SP 800-171, Revision2 controls; conduct an independent security assessment using NIST SP 800-171A, "*Assessing Security Requirements for Controlled Unclassified Information*" with results documented in a security assessment report; and security vulnerabilities or gaps in security requirements documented in a Plan of Action and Milestones. The resultant documents including the System Security Plan, Security Assessment Report, and Plan of Action and Milestones will be critical inputs to a risk management decision by the GSA to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the non-federal organization. The failure to implement the NIST SP 800-171, Revision 2 controls and maintain the supporting documentation will result in the termination of the contract. The non-federal system must have a new independent security assessment conducted at least every three (3) years or at the discretion of the GSA when there is a significant change to the system's security posture or via continuous monitoring. The contractor shall create, maintain and update the following security documentation and make available to the Government:

- **System Security Plan (SSP)** completed in agreement with NIST SP 800-171, Revision 2, "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*" using the template provided by the GSA.
- **Security Assessment Report (SAR)** completed in accordance with NIST SP 800-171A, "*Assessing Security Requirements for Controlled Unclassified Information*" using the template provided by the GSA. Nonfederal information systems must have an independent assessment performed and authorized every three (3) years or whenever there is a significant change to the non-federal system's security posture. The independent assessor shall be a FedRAMP accredited Third Party Assessment Organizations (3PAOs) or be approved by the GSA if not a 3PAO.
- **Plan of Action & Milestones** (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)*."
- **Penetration Test Report** (Not required; recommended only) documenting the results of an independent exercise. Reference GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

7.4 Reporting and Continuous Monitoring

Maintenance of security will be through continuous monitoring of security controls of the non-federal system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk

posture of the information system(s). They allow GSA to make credible risk-based decisions regarding the continued usage of non-federal systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided Quarterly to the GSA Information System Security Officer (ISSO), Information System Security Manager (ISSM), and/or Contracting Officer (COR)

1. Vulnerability Scanning
   Reference: NIST SP 800-171, Revision 2 Security Requirement 3.11.2
   Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. Provide the most recent Web Application and Operating System vulnerability scan reports.
2. Plan of Action & Milestones (POA&M) Update
   Reference: NIST SP 800-171, Revision 2 Security Requirement 3.12.2
   Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M)*."

Deliverables to be provided Annually or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Updated System Security Plan
   Reference: NIST 800-171, Revision 2 Security Requirement 3.12.4
   Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. The System Security Plan must be in accordance with NIST SP 800-171, Revision 2, using the Security Plan template provided by the GSA.

Deliverables to be provided every three years or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Security Assessment Report
   Reference: NIST 800-171, Revision 2 Security Requirement 3.12.1
   Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. Deliver the results of the security assessment conducted using the assessment procedures in NIST SP 800-171A, "*Assessing Security Requirements for Controlled Unclassified Information*", using the Security Assessment Report template provided by the GSA.

7.5 Privacy Assessment Activities and Required Documentation

Assessment of the privacy posture of the non-federal system and its environment of operation will be through continuous monitoring of privacy controls to determine if they remain effective

over time in light of changes that occur in the system and environment. Through continuous monitoring, privacy controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the privacy risk posture of the information system(s). They allow GSA to make credible risk-based decisions regarding the continued protection of CUI residents in non-federal systems and initiation of appropriate responses as needed when changes occur.

Deliverables to be provided Annually or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Privacy Threshold Assessment (PTA)
   Reference: NIST SP 800-171 Revision 2 Security Requirement 3.1.9 and 3.1.22
   The contractor shall prepare a PTA to confirm and document whether Personally Identifiable Information (PII) is in scope or not, and to determine which other categories of CUI will be stored, processed, or transmitted by the system. The PTA must be completed before GSA begins using the non-federal system.

   If through the initial PTA GSA finds that no PII or other CUI is in scope, then vendor shall both:
   a. Recertify the PTA on an annual basis to confirm the absence of such sensitive information; AND
   b. Update the PTA any time there is a change that may impact the privacy posture of the system or its environment of operation (e.g., collection of a new information type (see OMB Circular A-108, paragraph 6(b) for additional examples of significant changes requiring a PTA update).

Deliverables to be provided every three years or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Privacy Impact Assessment (PIA)
   Reference: NIST SP 800-171 Revision 2 Security Requirement 3.12.1[2]
   For any system that collects, maintains or disseminates PII or other CUI, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review. Then vendor shall:
   a. Limit system access to those with a Lawful Government Purpose; display login notifications or warning banners that CUI is present in the system and must be protected consistent with the CUI Program;
   b. Prohibit any CUI from being posted or processed on publicly accessible systems;
   c. Recertify the PIA every three years to confirm the collection, maintenance or dissemination of such sensitive information;

[2] NIST SP 800-53 provides guidance on security and privacy controls for systems and organizations.

d. Update the PIA any time there is a change that may impact the privacy posture of the system or its environment of operation (e.g., collection of a new information type (see OMB Circular A-108, paragraph 6(b) for additional examples of significant changes requiring a PIA update).

OMB's PIA guidance: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
GSA's PIA guidance: GSA Privacy Impact Assessment Guidance for Nonfederal Systems

- If PII is in scope, the vendor shall include the following NIST SP 800-53, Revision 4 Appendix J controls in its SSP. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII.

  AR-2 Privacy Impact and Risk Assessment
  AR-3 Privacy Requirements for Contractors and Service Providers
  AR-5(a) Privacy Awareness and Training
  AR-7 Privacy-Enhanced System Design and Development
  DI-1 Data Quality
  DM-1 Minimization of Personally Identifiable Information
  DM-3 Minimization of PII used in Testing, Training and Research
  IP-1 Consent
  IP-2(a) Individual Access
  IP-4 Complaint Management
  TR-1 Privacy Notice
  UL-1 Internal Use
  UL-2(a), (c), (d) Information Sharing with Third Parties

  The full text of each privacy control, along with their security counterparts, can be found in their entirety in NIST SP 800-53.

- A Privacy Policy/Notice shall be provided to users prior to their use of the application on what data is being collected and why, as well as the impact of not providing some or all of it. The Privacy Policy/Notice must be available to the individual directly on the form used to collect the information. Providing a link back to the Policy/Notice from the form is acceptable.

Other requirements: Government-approved terms of service.

7.6 Additional Stipulations

1. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or

is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

2. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system , unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

Appendix A: GSA Tailoring of NIST 800-53 Controls

The GSA Control Tailoring Workbook contains GSA defined values for NIST SP 800-53 Security and Privacy Controls. The workbook is not publicly available; contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.